Available online at www.sciencedirect.com
SCIENCE DIRECT

Journal of Combinatorial Theory, Series A 107 (2004) 143–146

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

Note

On a 5-design related to an extremal doubly even self-dual code of length 72

Masaaki Harada,[a,*] Masaaki Kitazume,[b] and Akihiro Munemasa[c]

[a] *Department of Mathematical Sciences, Yamagata University, Yamagata 990-8560, Japan*
[b] *Department of Mathematics and Informatics, Chiba University, Chiba 263-8522, Japan*
[c] *Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan*

Received 7 February 2004

Communicated by J.H. van Lint

Abstract

It is shown that if there is a self-orthogonal 5-(72,16,78) design, then the rows of its block-point incidence matrix generate an extremal doubly even self-dual code of length 72. In other words, a putative extremal doubly even self-dual code of length 72 is generated by the codewords of minimum weight.

Keywords: Self-orthogonal design; Binary code; Self-dual code

1. Introduction

A doubly even self-dual code of length 72 is called *extremal* if the minimum weight is 16 [2] and the existence of an extremal doubly even self-dual code of length 72 is a long-standing open question [4] (see also [3, Section 12]). It is known that the codewords of weight 16 in a putative extremal doubly even self-dual [72,36,16] code form a 5-(72,16,78) design $\mathscr{D}$ by the Assmus–Mattson theorem [1] (see also [3, Section 9]). A t-design is called *self-orthogonal* if the block intersection numbers have the same parity as the block size k [5]. The above 5-design $\mathscr{D}$ is self-orthogonal.

*Corresponding author.
E-mail address: harada@kdeve.kj.yamagata-u.ac.jp (M. Harada).

0097-3165/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2004.03.005

The aim of this note is to prove the following:

Theorem 1. *Let D be the code generated by the rows of a block-point incidence matrix of a self-orthogonal* 5-(72,16,78) *design* $\mathscr{D}$. *Then D is an extremal doubly even self-dual code of length* 72.

From Theorem 1 we immediately have the following:

Corollary 2. *The* 2*-rank of a self-orthogonal* 5-(72,16,78) *design is exactly* 36. *A putative extremal doubly even self-dual code of length* 72 *is generated by the codewords of minimum weight.*

2. A Proof of Theorem 1

For a t-(v,k,λ) design, every i-subset of points $(i \leqslant t)$ is contained in exactly $\lambda_i = \lambda\binom{v-i}{t-i}/\binom{k-i}{t-i}$ blocks. For a 5-(72,16,78) design, we have that

$$\lambda_0 = 249849, \quad \lambda_1 = 55522, \quad \lambda_2 = 11730, \quad \lambda_3 = 2346, \quad \lambda_4 = 442, \quad \lambda_5 = 78.$$

Let D be the code generated by the rows of a block-point incidence matrix A of a self-orthogonal 5-(72,16,78) design $\mathscr{D}$. Since the block size $k = 16$ is divisible by 4, D is a doubly even self-orthogonal code of length 72. Let $w \in D^{\perp}$ be a vector of weight $m > 0$, and let S be the support of w. Denote by n_i the number of rows of A intersecting exactly i positions of S in ones. Then we have the system of equations (cf. [5]):

$$\sum_{i=0}^{[m/2]} \binom{2i}{j} n_{2i} = \lambda_j \binom{m}{j} \quad (j = 0, 1, \ldots, 5). \tag{1}$$

Note that $n_{2i} = 0$ for $i \geqslant 9$. Then we have the following lemma.

Lemma 3. *The system of equations* (1) *has no solution under the assumption that* $n_{2i} = 0 \ (i \geqslant 5)$.

Proof. Solving the system of equations (1), we find $n_{10} = \alpha_{10} - 6n_{12} - 21n_{14} - 56n_{16}$ where

$$\begin{aligned}\alpha_{10} &= \frac{1}{1920}(3650496m - 800440m^2 + 67410m^3 - 2600m^4 + 39m^5)\\ &= \frac{m}{1920}\left(39\left(m^2 - \frac{100}{3}m + 275\right)^2 + \frac{7880}{3}\left(m - \frac{3204}{197}\right)^2 + \frac{1245957}{197}\right).\end{aligned} \tag{2}$$

For every $m > 0$, α_{10} cannot be 0. $\square$

We prove that every vector y in $D^{\perp}$ is contained in D by induction on $\mathrm{wt}(y)$, where $\mathrm{wt}(y)$ denotes the weight of y. First, note that the result is trivial for $y = 0$, so we may suppose that $\mathrm{wt}(y) > 0$. Then the system of equations (1) with $m = \mathrm{wt}(y)$ must have a solution $(n_0, n_2, \ldots)$. By Lemma 3, such a solution must have at least one of $n_{10}, n_{12}, \ldots$ nonzero. In particular, the minimum weight of D is at least 12. It also implies that there is a codeword x representing a block of the design, such that $\mathrm{wt}(x+y) < \mathrm{wt}(y)$. Since $x \in D \subset D^{\perp}$, we have $x + y \in D^{\perp}$. By induction, we obtain $x + y \in D$, and hence $y \in D$. In particular, if $\mathrm{wt}(y) = 12$, then $\mathrm{wt}(x+y) = 0$ is forced, which is a contradiction. Thus the minimum weight of D is 16. This completes the proof of Theorem 1.

Remark 4. Since D is doubly even and $D^{\perp}$ contains the all-one vector, it is sufficient to consider vectors $y \in D^{\perp}$ with $\mathrm{wt}(y) \equiv 0 \pmod 4$ and $\mathrm{wt}(y) \leqslant 36$.

Now we give an alternative proof.

Lemma 5. *The system of equations* (1) *has no solution* $(n_0, n_2, \ldots)$ *consisting of nonnegative integers for* $m \not\equiv 0 \pmod 4$.

Proof. The numerator of (2) cannot be divisible by 32 for $m \not\equiv 0 \pmod 4$. $\square$

By the above lemma, the dual code $D^{\perp}$ is doubly even. This means that $D^{\perp}$ is self-orthogonal. Hence D is self-dual. It remains to show that D has minimum weight 16. By Lemma 2.1(i) in [5], $D^{\perp}$ has minimum weight $\geqslant 6$. It follows from Lemma 3 that the system of equations (1) has no solution for $m = 8$, and one can easily check that (1) has no solution consisting of nonnegative integers for $m = 12$. Hence, $D^{\perp}$ contains no vector of weight 8 or 12. This completes the alternative proof of Theorem 1.

Proposition 6. *The block intersection numbers of a self-orthogonal* 5-(72,16,78) *design are exactly* $0, 2, 4, 6, 8$.

Proof. Let B be a block of $\mathscr{D}$ and let m_i be the number of other blocks which meet B in i points. Since the code D has minimum weight 16, $m_{10} = m_{12} = m_{14} = 0$. Then we have the system of equations:

$$\sum_{i=0}^{4} \binom{2i}{j} m_{2i} = (\lambda_j - 1)\binom{16}{j} \quad (j = 0, 1, \ldots, 5).$$

Then we have the following unique solution:

$$m_0 = 5082, \quad m_2 = 84480, \quad m_4 = 123480, \quad m_6 = 34496, \quad m_8 = 2310.$$

The result follows. $\square$

Acknowledgments

The authors would like to thank Vladimir Tonchev and the anonymous referee for their useful comments.

References

[1] E.F. Assmus Jr., H.F. Mattson Jr., New 5-designs, J. Combin. Theory 6 (1969) 122–151.
[2] C.L. Mallows, N.J.A. Sloane, An upper bound for self-dual codes, Inform. Control 22 (1973) 188–200.
[3] E. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 177–294.
[4] N.J.A. Sloane, Is there a $(72, 36)$ $d = 16$ self-dual code?, IEEE Trans. Inform. Theory 19 (1973) 251.
[5] V.D. Tonchev, A characterization of designs related to the Witt system S(5,8,24), Math. Z. 191 (1986) 225–230.